1995 年京大理 2

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}) = d$$

d は素数であり、a, b は自然数より、$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \geqq p > 1$であるから

$$a - b = 1 \quad \therefore a = b + 1 \quad d = (b+1)^p - b^p = {}_pC_{p-1}b^{p-1} + {}_pC_{p-2}b^{p-2} + \cdots + {}_pC_1 b + {}_pC_0$$

$$\therefore d - 1 = {}_pC_{p-1}b^{p-1} + {}_pC_{p-2}b^{p-2} + \cdots + {}_pC_1 b$$

ここで、二項係数 ${}_pC_m$ $(1 \leqq m \leqq p-1)$ について

$${}_pC_m = \frac{p!}{(p-m)!m!} = \frac{p}{m} \cdot \frac{(p-1)!}{(p-m)!(m-1)!} = \frac{p}{m} \cdot \frac{(p-1)!}{\{(p-1)-(m-1)\}!(m-1)!} = \frac{p}{m}\,{}_{p-1}C_{m-1}$$

$$\therefore m \cdot {}_pC_m = p \cdot {}_{p-1}C_{m-1}$$

p は素数であるから m は p の約数ではなく、${}_pC_m$ は p で割り切れる。
したがって、$d-1$ は p で割り切れる。

次に、$d = a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$ であり、a と b の奇偶は異なるので
$p-2$ 個の自然数 $a^{p-2}b, a^{p-3}b^2, \cdots, a^2b^{p-3}, ab^{p-2}$ は、いずれも偶数である。
a^{p-1} と b^{p-1} のうち、一方は奇数で、一方は偶数である。
したがって、d は奇数であり、$d-1$ は 2 で割り切れる。

以上により、$d-1$ は p でも 2 でも割り切れて、$p \neq 2$ であるから、$d-1$ は $2p$ で割り切れる。
すなわち、d を $2p$ で割った余りは 1 である。(証明終)